PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-077145
(43)Date of publication of application : 15.03.2002

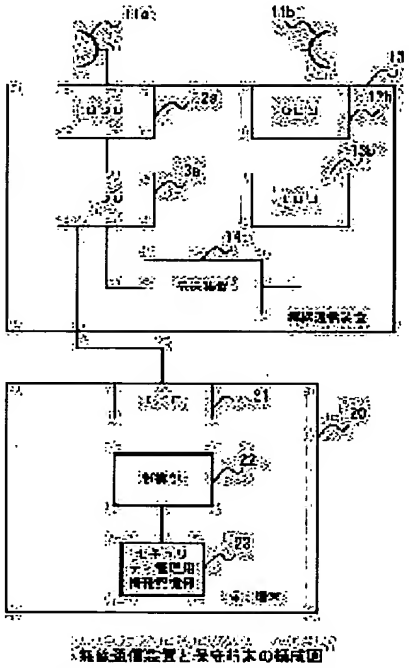
(51)Int.Cl. H04L 9/32
G06F 1/00

(21)Application number : 2000-259706
(22)Date of filing : 29.08.2000

(71)Applicant : TOSHIBA CORP
(72)Inventor : HOSAKA MITSURU

(54) SECURITY MANAGING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To realize security of maintenance and supervisory of communication system or the like with simple constitution.
SOLUTION: When a maintenance terminal 20 is connected with radio equipment 10, information for security management of the terminal 20 and that of the radio equipment 10 are compared with each other. When coincidence is obtained, the terminal 20 is so controlled that operation is possible. When coincidence is not obtained, the terminal 20 is so controlled that operation is not possible.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００２－７７１４５

(Ｐ２００２－７７１４５Ａ)

(43)公開日　平成14年3月15日(2002.3.15)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	1/00	３７０　Ｅ	5J104
Ｇ０６Ｆ	1/00	３７０	Ｈ０４Ｌ	9/00	６７５　Ａ	
					６７３　Ｂ	

審査請求　未請求　請求項の数５　ＯＬ　(全８頁)

(21)出願番号　特願2000-259706(P2000-259706)

(22)出願日　平成12年8月29日(2000.8.29)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目1番1号

(72)発明者　保坂　充
東京都日野市旭が丘3丁目1番地の1　株式会社東芝日野工場内

(74)代理人　100071054
弁理士　木村　高久

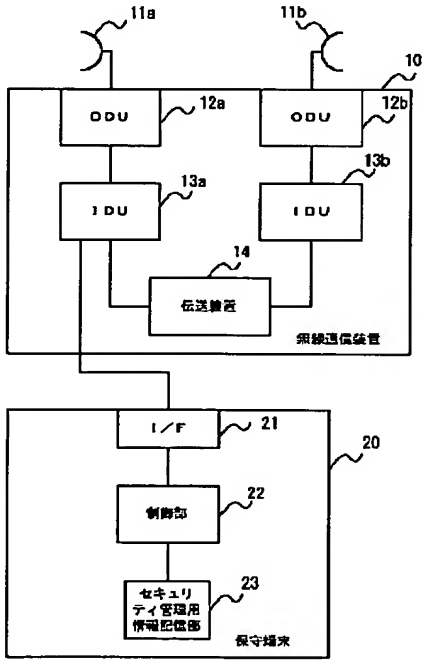
Ｆターム(参考)　5J104 AA07 KA02 KA04 NA05

(54)【発明の名称】セキュリティ管理方法

(57)【要約】

【課題】　通信システム等の保守、監視のセキュリティを簡単な構成により実現する。

【解決手段】　無線装置１０に保守端末２０が接続された時点で互いのセキュリティ管理用情報を比較し、一致していれば、この保守端末２０の動作を可能にし、不一致であれば、この保守端末２０を動作不可に制御する。



無線通信装置と保守端末の構成図

1

【特許請求の範囲】

【請求項１】　据付型の第１の装置に対して可搬型の第２の装置を接続して前記第１の装置のデータ設定を行うシステムにおけるセキュリティ管理方法において、

前記第１の装置および前記第２の装置にそれぞれにセキュリティ管理用情報を記憶し、

前記第１の装置に対する前記第２の装置の接続に際して、前記第１の装置および前記第２の装置間で前記セキュリティ管理用情報の照合を行い、

該照合結果に基づき前記第１の装置に対する前記第２の装置によるデータ設定を許可することを特徴とするセキュリティ管理方法。

【請求項２】　前記第１の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶された前記第２の装置を接続した場合は、前記第２の装置のセキュリティ管理用情報を用いて前記第１の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第１の装置に対する前記第２の装置によるデータ設定を可能にしたことを特徴とする請求項１記載のセキュリティ管理方法。

【請求項３】　前記第１の装置に前記セキュリティ管理用情報が記憶されていない前記第２の装置を接続した場合は、前記第１の装置のセキュリティ管理用情報を用いて前記第２の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第１の装置に対する前記第２の装置によるデータ設定を可能にしたことを特徴とする請求項１記載のセキュリティ管理方法。

【請求項４】　前記第１の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶されていない前記第２の装置を接続した場合は、前記第１の装置および前記第２の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第１の装置に対する前記第２の装置によるデータ設定を可能にしたことを特徴とする請求項１記載のセキュリティ管理方法。

【請求項５】　前記第１の装置は、

通信システムを構成する複数の通信装置の内の１つの通信装置であり、

前記第２の装置は、

前記通信システムの保守、管理を行う保守端末であることを特徴とする請求項１記載のセキュリティ管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信システム等の保守、管理のセキュリティを実現するセキュリティ管理方法に関する。

【０００２】

【従来の技術】従来、据付型の複数の無線通信装置から構成される通信システムの全体の監視、制御は、上記複数の無線通信装置のいずれかに接続された監視制御装置

2

（ＮＭＳ）により行われている。

【０００３】また、上記通信システムの複数の無線通信装置を個別に設定、保守するする場合は、制御対象となる無線通信装置に可搬型の保守端末を接続することにより行われている。

【０００４】例えば、上記通信システムの複数の無線通信装置うちの特定の無線通信装置の警報状態を調べる場合、若しくは、上記無線通信装置の装置名称等を設定する場合、若しくは、上記無線通信装置の使用周波数を設定する場合、若しくは、上記無線通信装置の警報出力論理を設定する場合、若しくは、上記無線通信装置のログイン名またはパスワード等を個別に設定する場合は、当該無線通信装置に上記可搬型の保守端末を接続して、この保守端末を用いてこの通信システムの各種情報の監視若しくは設定を行う。

【０００５】

【発明が解決しようとする課題】ところで、上記保守端末は、特定の通信システムに対応して設計、開発されており、例えば、この保守端末を誤って他の通信システムの無線通信装置に接続した場合、若しくは故意に他の通信システムの無線通信装置に接続した場合は、この他の通信システムの無線通信装置の情報を誤って変更してしまったり、他の通信システムの無線通信装置の情報を不当に収集してしまったりするという事態が発生した。

【０００６】例えば、ある通信システムにおける無線通信装置の増設時に、この通信システムとは異なる通信システムのために開発された保守端末をこの増設した無線通信装置に接続して、各種設定を行った場合は、この増設した無線通信装置にこの通信システムに許可されていない周波数を設定してしまうことがあり、この場合は、通信システム間で混信が発生するという問題があり、また、不当に他の通信システムの情報が収集されてしまうという問題が発生し、これにより通信システム間のセキュリティが保てないという問題が発生した。

【０００７】そこで、この発明は、通信システム等の保守、監視のセキュリティを簡単な構成により実現することを可能にしたセキュリティ管理方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】この発明のセキュリティ管理方法は、据付型の第１の装置に対して可搬型の第２の装置を接続して前記第１の装置のデータ設定を行うシステムにおけるセキュリティ管理方法において、前記第１の装置および前記第２の装置にそれぞれにセキュリティ管理用情報を記憶し、前記第１の装置に対する前記第２の装置の接続に際して、前記第１の装置および前記第２の装置間で前記セキュリティ管理用情報の照合を行い、該照合結果に基づき前記第１の装置に対する前記第２の装置によるデータ設定を許可することを特徴とする。

【０００９】すなわち、この発明のセキュリティ管理方法によれば、第１の装置に第２の装置が接続された時点で互いのセキュリティ管理用情報を比較し、一致していれば第１の装置および第２の装置が１つのシステムとして動作し、不一致であれば、第１の装置および第２の装置は１つのシステムとしては動作しない。

【００１０】このような構成によると、２つの装置を接続した時点でそれぞれの装置が当該システムのために設置した装置であるかどうかが判別可能になり、例えば、他のシステムでの使用のための装置を持ち込んでシステムに組み込む不正使用を防止することができ、システムのセキュリティを確保することができる。

【００１１】また、この発明のセキュリティ管理方法は、前記第１の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶された前記第２の装置を接続した場合は、前記第２の装置のセキュリティ管理用情報を用いて前記第１の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第１の装置に対する前記第２の装置によるデータ設定を可能にしたことを特徴とする。

【００１２】また、この発明のセキュリティ管理方法は、前記第１の装置に前記セキュリティ管理用情報が記憶されていない前記第２の装置を接続した場合は、前記第１の装置のセキュリティ管理用情報を用いて前記第２の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第１の装置に対する前記第２の装置によるデータ設定を可能にしたことを特徴とする。

【００１３】また、この発明のセキュリティ管理方法は、前記第１の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶されていない前記第２の装置を接続した場合は、前記第１の装置および前記第２の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第１の装置に対する前記第２の装置によるデータ設定を可能にしたことを特徴とする。

【００１４】すなわち、第１の装置と第２の装置のセキュリティ管理用情報を比較したときに一方のセキュリティ管理用情報が未設定である場合は、設定済みのセキュリティ管理用情報を使って未設定のセキュリティ管理用情報を若しくは両者のセキュリティ管理用情報を自動的に設定する。

【００１５】このような構成によると、装置故障や装置の増設対応などにより、新しく装置をシステムに組み込む場合には、自動的にセキュリティ管理用情報の設定が行われるので、システム構築を迅速に行うことができる。

【００１６】

【発明の実施の形態】以下、この発明に係わるセキュリティ管理方法の実施の形態を添付図面を参照して詳細に説明する。

【００１７】図１は、この発明に係わるセキュリティ管理方法を適用する通信システムの一例を示すシステム構成図である。

【００１８】この通信システムは、複数台、図１においては４台の無線通信装置１０－１～１０－４を無線回線でリング状に接続して構成される。

【００１９】また、４台の無線通信装置１０－１～１０－４の内の無線通信装置１０－３には、この通信システムの全体の監視、制御を行う監視制御装置（ＮＭＳ）１００が接続されている。

【００２０】また、図１においては、この通信システムを構成する無線通信装置１０－１～１０－４のうちの無線通信装置１０－４を個別に調整若しくは保守のために、この無線通信装置１０－４に保守端末２０を接続した場合を示している。

【００２１】なお、図１においては、保守端末２０を無線通信装置１０－４に接続した場合を示しているが、この保守端末２０は、他の無線通信装置１０－１～１０－３にも同様に接続することができる。

【００２２】図２は、図１に示した無線通信装置１０－１～１０－４および保守端末２０の構成を示すブロック図である。

【００２３】なお、図２において、無線通信装置１０は、図１に示した無線通信装置１０－１～１０－４の内の１台の無線通信装置を示している。

【００２４】図２において、この無線通信装置１０は、アンテナ１１ａ，１１ｂ、アンテナ１１ａ，１１ｂにそれぞれ接続され、主に屋外に設置されるＯＤＵ（アウトドアユニット）１２ａ，１２ｂ、ＯＤＵ１２ａ，１２ｂにそれぞれ接続され、主に屋内に設置されて主に無線通信のベースバンド信号の処理およびＯＤＵ１２ａ，１２ｂの制御を行うＩＤＵ（インドアユニット）１３ａ，１３ｂ、ＩＤＵ１３ａ，１３ｂに接続される伝送装置１４を具備して構成される。

【００２５】ここで、伝送装置１４は、例えば、ＡＴＭ伝送装置を用いて構成されており、予め設定された通信パスに基づきＩＤＵ１３ａ，１３ｂ間の伝送情報をスルーしたり、この伝送装置１４に接続された図示しない端末に出力したりする動作を行う。ここで、ＡＴＭの場合の通信パスの設定とはＶＯＩ／ＶＣＩ毎に伝送情報をどのポートに出力するかの設定を行う。なお、この伝送装置１４としては、ＡＴＭ伝送装置に限らず、例えば、ＳＤＨ方式等の同期多重方式を用いた伝送装置を採用することもできる。

【００２６】なお、図２の構成において、保守端末２０は、ＩＤＵ１３ａ若しくは１３ｂに接続されるが、図２においては、保守端末２０をＩＤＵ１３ａに接続した場合を示している。

【００２７】すなわち、図２において、ＩＤＵ１３ａ，１３ｂは、図３に示しように構成されている。

【００２８】図３は、図２に示したＩＤＵ１３ａ，１３ｂをＩＤＵ１３として示すもので、ＯＤＵ１２ａ若しくは１２ｂに接続されるとともに、伝送装置１４に接続される送信部１３１および受信部部１３２、この送信部１３１および受信部部１３２を制御するとともに、このＩＤＵ１３の全体動作を制御する制御部１３３、この発明に係わるセキュリティ管理情報を記憶するセキュリティ管理情報菊部１３４、図２に示した保守端末２０との通信のインタフェースをなす保守端末用インタフェース（保守端末用Ｉ／Ｆ）１３５を具備して構成される。

【００２９】さて、図２において、保守端末２０は、無線通信装置１０（ＩＤＵ１３ａ）との通信のインタフェースをなすインタフェース部（Ｉ／Ｆ）２１、この保守端末２０の全体動作を統括制御する制御部２２、この発明に係わるセキュリティ管理用情報を記憶するセキュリティ管理用情報記憶部２３を具備して構成される。

【００３０】ここで、保守端末２０は、図１に示した通信システムの各無線通信装置１０－１～１０－４の各種情報を個別に設定、保守するもので、この通信システムのために専用に開発されたものである。

【００３１】この保守端末２０の設定監視動作としては、

１）無線通信装置の警報状態
２）無線通信装置の装置名称等の設定
３）無線通信装置の使用周波数の設定
４）無線通信装置の警報出力論理
５）無線通信装置のログイン名またはパスワード等の設定

等を行う。

【００３２】なお、この実施の形態においては、無線通信装置１０のＩＤＵ１３ａのセキュリティ管理用情報記憶部１３４に記憶されているセキュリティ管理用情報と保守端末２０のセキュリティ管理用情報記憶部２３に記憶されているセキュリティ管理用情報とは同一の情報が使用されているが、保守端末２０がこの無線通信装置１０により構築される通信システムのために開発されたものであることが識別できれば、ＩＤＵ１３ａのセキュリティ管理用情報記憶部１３４に記憶されているセキュリティ管理用情報と保守端末２０のセキュリティ管理用情報記憶部２３に記憶されているセキュリティ管理用情報とは同一でなくてもよい。

【００３３】また、無線通信装置１０のセキュリティ管理用情報記憶部１３４に記憶されているセキュリティ管理用情報および保守端末２０のセキュリティ管理用情報記憶部２３に記憶されているセキュリティ管理用情報は、セキュリティの程度に応じて任意の情報量、任意の形態の情報を使用することができる。

【００３４】また、無線通信装置の使用周波数、すなわち、この場合、ＯＤＵ１２ａの無線周波数の設定は、ＩＤＵ１３ａを介して設定される。

【００３５】図４は、図２に示した保守端末２０の動作を説明するフローチャートである。

【００３６】図４において、この保守端末２０は、まず、無線通信装置１０に接続されたかを調べる（ステップ３０１）。ここで、無線通信装置１０に接続されていないと判断されると、ステップ３０１に戻り、無線通信装置１０に接続されるのを待つ。

【００３７】ステップ３０１で、無線通信装置１０に接続されたと判断されると（ステップ３０１でＹＥＳ）、無線通信装置１０のセキュリティ管理用情報記憶部１３４からセキュリティ管理用情報を取り出し（ステップ３０２）、無線通信装置１０のセキュリティ管理用情報記憶部１３４にはセキュリティ管理用情報が設定済かを調べる（ステップ３０３）。

【００３８】ここで、無線通信装置１０のセキュリティ管理用情報記憶部１３４にセキュリティ管理用情報が設定済であると判断されると（ステップ３０３でＹＥＳ）、次に、保守端末２０のセキュリティ管理用情報記憶部２３からセキュリティ管理用情報を取り出す（ステップ３０４）。

【００３９】そして、保守端末２０のセキュリティ管理用情報記憶部２３にはセキュリティ管理用情報が設定済かを調べる（ステップ３０５）。ここで、保守端末２０のセキュリティ管理用情報記憶部２３にセキュリティ管理用情報が設定済であると判断されると（ステップ３０５でＹＥＳ）、無線通信装置１０のセキュリティ管理用情報記憶部１３４から取り出したセキュリティ管理用情報と保守端末２０のセキュリティ管理用情報記憶部２３から取り出したセキュリティ管理用情報とを比較する（ステップ３０６）。

【００４０】この比較において、無線通信装置１０のセキュリティ管理用情報記憶部１３４から取り出したセキュリティ管理用情報と保守端末２０のセキュリティ管理用情報記憶部２３から取り出したセキュリティ管理用情報とが一致すると（ステップ３０６で一致）、この保守端末２０は、この通信システムにに組み込み可能であると判断して、この保守端末２０の使用中状態となる（ステップ３０７）。

【００４１】そして、次に、無線通信装置１０との接続が断かを調べ（ステップ３０８）、接続断でないと判断されると（ステップ３０８でＮＯ）、ステップ３０７に戻り、この保守端末２０の使用中状態を続ける。

【００４２】また、ステップ３０８で、無線通信装置１０との接続が断であると判断されると（ステップ３０８でＹＥＳ）、この保守端末２０の使用中状態を終了してステップ３０１へ戻る。

【００４３】また、ステップ３０６で、無線通信装置１０のセキュリティ管理用情報記憶部１３４から取り出したセキュリティ管理用情報と保守端末２０のセキュリティ管理用情報記憶部２３から取り出したセキュリティ管

理用情報とが一致しないと判断されると（ステップ３０６で不一致）、この保守端末２０は、この通信システムにに組み込み不可であると判断して、この保守端末２０の使用不可状態となる（ステップ３０９）。

【００４４】そして、次に、無線通信装置１０との接続が断かを調べ（ステップ３１０）、接続断でないと判断されると（ステップ３１０でＮＯ）、ステップ３０９に戻り、この保守端末２０の使用不可状態を続けるが、ステップ３１０で、無線通信装置１０との接続が断であると判断されると（ステップ３１０でＹＥＳ）、ステップ３０１へ戻る。

【００４５】また、ステップ３０３で、無線通信装置１０のセキュリティ管理用情報記憶部１３４にセキュリティ管理用情報が設定されていないと判断されると（ステップ３０３でＮＯ）、次に、保守端末２０のセキュリティ管理用情報記憶部２３からセキュリティ管理用情報を取り出し（ステップ３１１）、保守端末２０のセキュリティ管理用情報記憶部２３にはセキュリティ管理用情報が設定済かを調べる（ステップ３１２）。

【００４６】ここで、保守端末２０のセキュリティ管理用情報記憶部２３にセキュリティ管理用情報が設定済であると判断されると（ステップ３１２でＹＥＳ）、未設定の無線通信装置１０のセキュリティ管理用情報記憶部１３４に保守端末２０のセキュリティ管理用情報記憶部２３に設定されているセキュリティ管理用情報を設定し（ステップ３１３）、保守端末２０の使用中状態となる（ステップ３０７）。

【００４７】すなわち、保守端末２０のセキュリティ管理用情報記憶部２３にはセキュリティ管理用情報が設定されているが、無線通信装置１０のセキュリティ管理用情報記憶部１３４にはセキュリティ管理用情報が設定されていない場合は、設定済みの保守端末２０のセキュリティ管理用情報記憶部２３に記憶されたセキュリティ管理用情報を用いて未設定の無線通信装置１０のセキュリティ管理用情報記憶部１３４にセキュリティ管理用情報を自動設定して、保守端末２０の使用を可能にする。

【００４８】また、ステップ３１２で、保守端末２０のセキュリティ管理用情報記憶部２３にセキュリティ管理用情報が設定されていないと判断されると（ステップ３１２でＮＯ）、この場合は、無線通信装置１０のセキュリティ管理用情報記憶部１３４および保守端末２０のセキュリティ管理用情報記憶部２３に新たなセキュリティ管理用情報を自動設定して保守端末２０の使用中状態となる（ステップ３０７）。

【００４９】すなわち、無線通信装置１０のセキュリティ管理用情報記憶部１３４および保守端末２０のセキュリティ管理用情報記憶部２３にそれぞれセキュリティ管理用情報が設定されていない場合は、無線通信装置１０のセキュリティ管理用情報記憶部１３４および保守端末２０のセキュリティ管理用情報記憶部２３にそれぞれ新たなセキュリティ管理用情報を自動設定して、保守端末２０の使用を可能にする。

【００５０】また、ステップ３０５で、保守端末２０のセキュリティ管理用情報記憶部２３にセキュリティ管理用情報が設定されていないと判断されると（ステップ３０５でＮＯ）、未設定の保守端末２０のセキュリティ管理用情報記憶部２３に無線通信装置１０のセキュリティ管理用情報記憶部１３４に設定されているセキュリティ管理用情報を設定し、保守端末２０の使用中状態となる（ステップ３０７）。

【００５１】すなわち、無線通信装置１０のセキュリティ管理用情報記憶部１３４にはセキュリティ管理用情報が設定されているが、保守端末２０のセキュリティ管理用情報記憶部２３にはセキュリティ管理用情報が設定されていない場合は、設定済みの無線通信装置１０のセキュリティ管理用情報記憶部１３４に記憶されたセキュリティ管理用情報を用いて未設定の保守端末２０のセキュリティ管理用情報記憶部２３にセキュリティ管理用情報を自動設定して、保守端末２０の使用を可能にする。

【００５２】このような構成によると、無線通信装置１０に保守端末２０を接続した時点で保守端末２０が当該通信システムのための装置であるかどうかが判別可能になり、例えば、他の通信システムでの使用のための装置を持ち込んでこの通信システムに組み込む不正使用を防止することができ、通信システムのセキュリティを確保することができる。

【００５３】また、無線通信装置１０と保守端末２０のセキュリティ管理用情報を比較したときに一方のセキュリティ管理用情報が未設定である場合は、設定済みのセキュリティ管理用情報を使って未設定のセキュリティ管理用情報を若しくは両者のセキュリティ管理用情報を自動的に設定するように構成したので、装置故障や装置の増設対応などにより、新しく装置をこの通信システムに組み込む場合には、自動的にセキュリティ管理用情報の設定が行われるので、システム構築を迅速に行うことができる。

【００５４】図５は、図２に示した無線通信装置１０に保守端末２０を接続した場合に、保守端末２０と無線通信装置１０との間で行われる信号シーケンスの一例を示す図である。

【００５５】図５において、保守端末２０が無線通信装置１０に接続されると、保守端末２０から無線通信装置１０へデータ表示要求が送信される。

【００５６】このデータ表示要求を受信した無線通信装置１０は、保守端末２０へこのデータ表示要求に対するデータ表示応答を返信する。

【００５７】これにより、保守端末２０では、無線通信装置１０からの表示情報を表示することが可能になる。

【００５８】図６は、図２に示した無線通信装置１０に保守端末２０を接続した場合に、保守端末２０と無線通

信装置１０との間で行われる信号シーケンスの他の例を示す図である。

【００５９】図６においては、図５に示した、保守端末２０から無線通信装置１０へのデータ表示要求の送信および無線通信装置１０から保守端末２０へのデータ表示応答の返信に加えて、保守端末２０から無線通信装置１０へのデータ設定要求の送信および無線通信装置１０から保守端末２０へのデータ設定応答の返信が可能になるように構成されている。

【００６０】このような構成によると、保守端末２０では、無線通信装置１０からの表示情報の表示だけでなく、無線通信装置１０に対するデータ設定が可能になる。

【００６１】なお、上述した実施の形態においては、この発明を通信システムに適用した場合を示したが、この発明に係わるセキュリティ管理方法は、上述したような通信システムに限らず、セキュリティ管理の必要な他のシステムにも同様に適用することができる。

【００６２】また、この発明は上述した実施の形態の構成に限定されず、その他、この発明の要旨を逸脱しない範囲で種々の変形を施しても同様に実施可能であることは言うまでもない。

【００６３】

【発明の効果】以上説明したようにこの発明によれば、第１の装置に第２の装置が接続された時点で互いのセキュリティ管理用情報を比較し、一致していれば１つのシステムとして動作し、不一致であれば、１つのシステムとしては動作しないように構成したので、２つの装置を接続した時点でそれぞれの装置が当該システムのために設置した装置であるかどうかが判別可能になり、例えば、他のシステムでの使用のための装置を持ち込んでシステムに組み込む不正使用を防止することができ、システムのセキュリティを確保することができる。

【００６４】また、第１の装置と第２の装置のセキュリティ管理用情報を比較したときに一方のセキュリティ管理用情報が未設定である場合は、設定済みのセキュリティ管理用情報を使って未設定のセキュリティ管理用情報を若しくは両者のセキュリティ管理用情報を自動的に設定するように構成したので、装置故障や装置の増設対応などにより、新しく装置をシステムに組み込む場合には、自動的にセキュリティ管理用情報の設定が行われるので、システム構築を迅速に行うことができる。

【図面の簡単な説明】

【図１】この発明に係わるセキュリティ管理方法を適用する通信システムの一例を示すシステム構成図である。

【図２】図１に示した無線通信装置および保守端末の構成を示すブロック図である。

【図３】図２に示したＩＤＵの詳細構成を示すブロック図である。

【図４】図２に示した保守端末２０の動作を説明するフローチャートである。

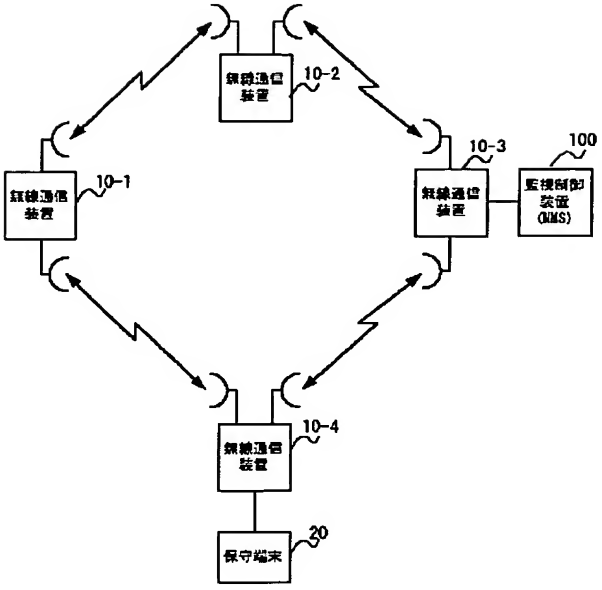
【図５】図２に示した無線通信装置１０に保守端末２０を接続した場合に、保守端末２０と無線通信装置１０との間で行われる信号シーケンスの一例を示す図である。

【図６】図２に示した無線通信装置１０に保守端末２０を接続した場合に、保守端末２０と無線通信装置１０との間で行われる信号シーケンスの他の例を示す図である。

【符号の説明】

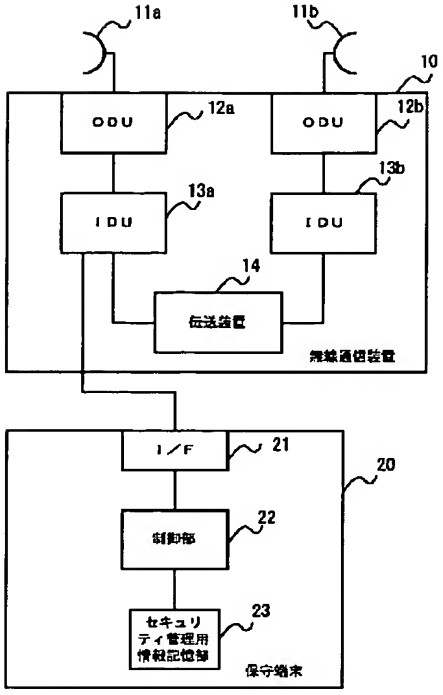
１０、１０－１～１０－４　　無線通信装置
１１ａ，１１ｂ　　アンテナ
１２ａ，１２ｂ　　ＯＤＵ（アウトドアユニット）
１３，１３ａ，１３ｂ　　ＩＤＵ（インドアユニット）
１４　　伝送装置
２０　　保守端末
２１　　インタフェース（Ｉ／Ｆ）
２２　　制御部
２３　　セキュリティ管理用情報記憶部
１００　　監視制御部（ＮＭＳ）
１３１　　送信部
１３２　　受信部
１３３　　制御部
１３４　　セキュリティ管理用情報記憶部
１３５　　保守端末用インタフェース（保守端末用Ｉ／Ｆ）

【図１】



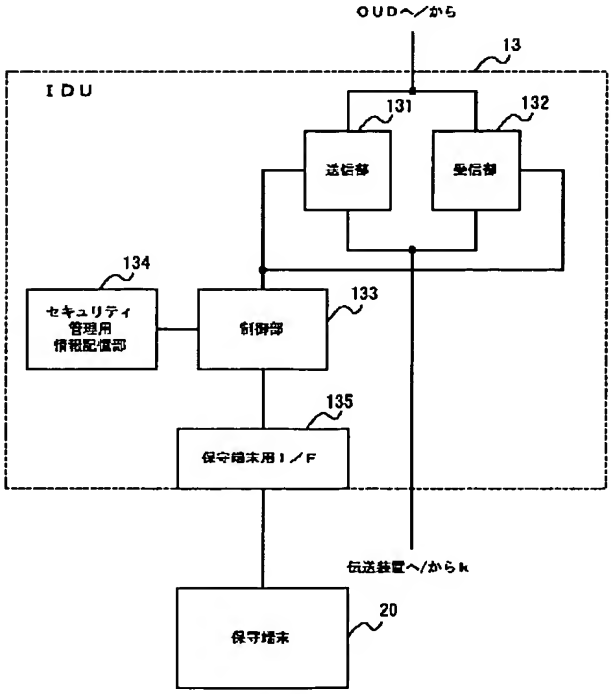
全体構成

【図２】



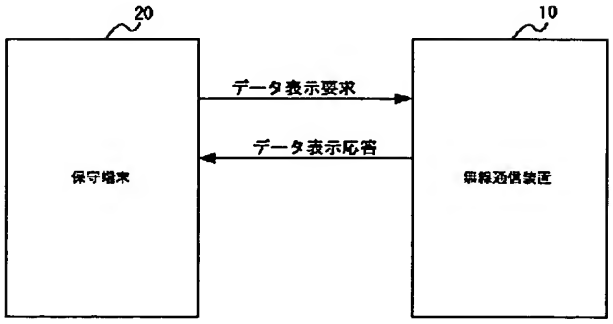
無線通信装置と保守端末の構成図

【図３】



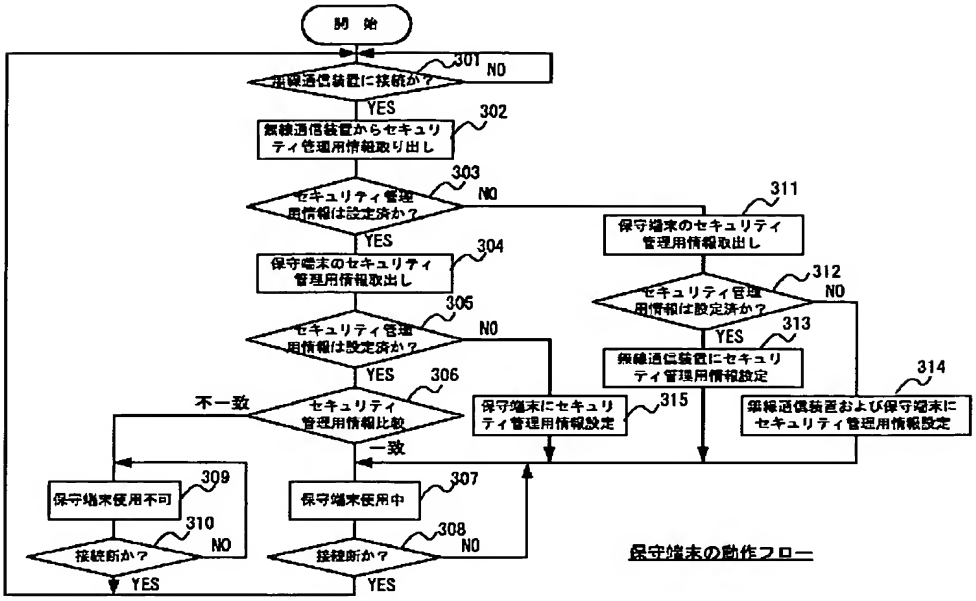
IDUの構成図

【図５】



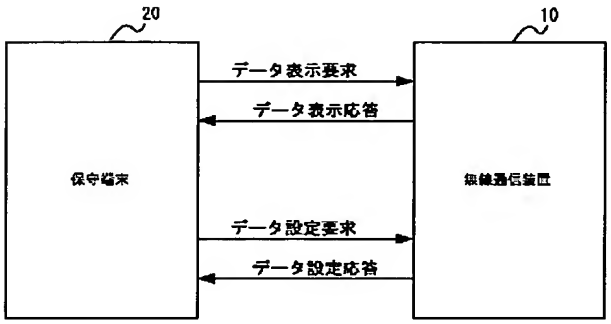
保守端末と無線通信装置との間の信号シーケンス図

【図４】



保守端末の動作フロー

【図６】



保守端末と無線通信装置との間の他の信号シーケンス図